

(19) 日本国特許庁 (J P)

(12) 特 許 公 報 (B 2)

(11) 特許番号

第2937919号✓

(45) 発行日 平成11年(1999) 8月23日

(24) 登録日 平成11年(1999) 6月11日

(51) Int.Cl.⁶

識別記号

F I

G 0 6 F 7/58

G 0 6 F 7/58

A

G 0 9 C 1/00

6 5 0

G 0 9 C 1/00

6 5 0 B

H 0 3 K 3/84

H 0 3 K 3/84

A

請求項の数 3 (全 7 頁)

(21) 出願番号

特願平9-5335

(22) 出願日

平成9年(1997) 1月16日

(65) 公開番号

特開平10-207695

(43) 公開日

平成10年(1998) 8月7日

審査請求日

平成9年(1997) 1月16日

(73) 特許権者 000232036

日本電気アイシーマイコンシステム株式
会社

神奈川県川崎市中原区小杉町1丁目403
番53

(72) 発明者

田中 正則

神奈川県川崎市中原区小杉町1丁目403
番53 日本電気アイシーマイコンシステ
ム株式会社内

(72) 発明者

石本 淳一

神奈川県川崎市中原区小杉町1丁目403
番53 日本電気アイシーマイコンシステ
ム株式会社内

(74) 代理人

弁理士 山川 政樹

審査官

石田 信行

最終頁に続く

(54) 【発明の名称】 疑似乱数発生回路

1

(57) 【特許請求の範囲】

【請求項1】 直列に接続された複数のレジスタの所定の出力が排他的論理和回路を介して先頭のレジスタにフィードバックされるリニアフィードバックシフトレジスタを用いた疑似乱数発生回路において、生成する乱数のビット幅分のレジスタと少なくとも1ビットの冗長レジスタから前記複数のレジスタが構成され、シフトクロックに応じてシフト動作を行うリニアフィードバックシフトレジスタと、
冗長レジスタの出力値に応じて複数の内部クロックから1つを選択し、これを前記シフトクロックとして出力する選択回路とを有することを特徴とする疑似乱数発生回路。

【請求項2】 直列に接続された複数のレジスタの所定の出力が排他的論理和回路を介して先頭のレジスタにフ

2

ィードバックされるリニアフィードバックシフトレジスタを用いた疑似乱数発生回路において、生成する乱数のビット幅分のレジスタと少なくとも1ビットの冗長レジスタから前記複数のレジスタが構成され、シフトクロックに応じてシフト動作を行うリニアフィードバックシフトレジスタと、
冗長レジスタの出力値に応じて複数の内部クロックから1つを選択する選択回路と、
前記内部クロックよりも高速なクロックと選択回路の出力との論理積をとり、この結果を前記シフトクロックとして出力する論理積回路とを有することを特徴とする疑似乱数発生回路。

【請求項3】 請求項1又は2記載の疑似乱数発生回路において、
前記リニアフィードバックシフトレジスタの代わりに、

3

生成する乱数のビット幅分のレジスタから前記複数のレジスタが構成され、シフトクロックに応じてシフト動作を行う第1のリニアフィードバックシフトレジスタと、複数のレジスタ中に少なくとも1ビットの冗長レジスタを含み、シフトクロックに応じてシフト動作を行う第2のリニアフィードバックシフトレジスタとを有することを特徴とする疑似乱数発生回路。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、LFSRを用いた疑似乱数発生回路に係り、特に乱数の周期に不規則性を持たせて乱数性を高めた疑似乱数発生回路に関するものである。

【0002】

【従来の技術】従来より、暗号アルゴリズム等に乱数が用いられているが、このときの乱数としては、扱いやすさや処理の簡単さから真性乱数よりも、ソフトウェアでも容易に作成可能な疑似乱数を用いることが多い。疑似乱数を発生する疑似乱数発生回路としては、リニアフィードバックシフトレジスタ（Linear Feedback Shift Register、以下、LFSRと略す）が生成する長周期の乱数列を用いることが一般的となっている。LFSRは、直列に接続された複数のレジスタの所定の出力が排他的論理和回路を介して先頭のレジスタにフィードバックされる構造となっており、フィードバック部に排他的論理和回路を設けることにより、比較的長周期の乱数列を得ることが可能である。

【0003】例えば、 n 個のレジスタで構成されるLFSRから得られる乱数列の周期は、 n 次の線形最大周期列（M系列と呼ばれる） $2^n - 1$ となる。なお、LFSRで用いられる周期とは、時間を表すものではなく、生成される乱数のパターンが何通りあるかを示すパターン周期（つまり、このパターン周期ごとに同一の乱数が発生する）であるが、以降では単に周期と記載する。図5に7段のLFSRを用いた従来の疑似乱数発生回路のブロック図を示す。この疑似乱数発生回路は、直列に接続された七個のレジスタ12-1～12-7のうちの2段目のレジスタ12-2の出力と最後段のレジスタ12-7の出力を排他的論理和回路14に入力し、この排他的論理和回路14の出力を先端のレジスタ12-1の入力にフィードバックする構成となっている。

【0004】LFSRを用いた疑似乱数発生回路の場合、M系列のビット列を生成するので、図5のような7段のLFSRの場合は、127（ $=2^7 - 1$ ）通りの疑似乱数列を生成することができる。このような n 段の構造を持つLFSRは、 $2^n - 1$ の周期を有する乱数列が得られるものであるが、生成される乱数列を暗号回路のシードとして用いた場合、この暗号回路から生成される暗号文は比較的容易に解読されてしまう危険性がある。例えば、畳み込み符号に代表されるストリーム型暗号で

4

は、平文の2進系列と疑似乱数発生回路から生成した2進疑似乱数系列の排他的論理和をとることによりストリーム暗号を生成するが、疑似乱数系列又は疑似乱数系列生成論理が判明してしまった場合、入手した暗号文から平文を再生することは容易に可能であり、その結果暗号回路としての機能を失ってしまうことになる。

【0005】暗号回路から出力される暗号文のデータ解析等を行っても、予測不可能な疑似乱数系列を効率的に生成することが重要なことは周知の事実である。データ解析を行っても解析不可能な疑似乱数系列を生成するには、次数 n （レジスタの個数）を増やせばよいが、回路規模等の制約から少ないビット数のLFSRしか使用することができない場合がある。したがって、少ないビット数のLFSRを用いた疑似乱数発生回路から生成される乱数列を暗号アルゴリズムのシードとして用いる場合には、乱数列の予測が困難となるように効率的に乱数列の周期を乱す工夫が必要となる。

【0006】そこで、少ないビット数のLFSRで乱数性を高めた疑似乱数発生回路が提案されている（特開平5-327427号公報）。図6、図7に特開平5-327427号公報で提案された従来の疑似乱数発生回路のブロック図を示す。図6の疑似乱数発生回路では、先頭のレジスタ12-1の出力と最後段のレジスタ12-7の出力を排他的論理和回路14aに入力している。そして、切替スイッチ15は、この排他的論理和回路14aの出力とレジスタ12-7の出力のうちの何れかを選択して、レジスタ12-1の入力にフィードバックするように接続されている。この切替スイッチ15は、通常、排他的論理和回路14aの出力を選択しており、レジスタ12-1～12-7のビット数に応じた乱数列の一周期分の回数だけLFSRがシフトした後に、レジスタ12-7の出力を選択し、この状態で所定の回数のシフトが行われた後に、再び排他的論理和回路14aの出力を選択する。このようにして、乱数列の周期を長くすることができる。

【0007】また、図7の疑似乱数発生回路では、先頭のレジスタ12-1の出力と2段目のレジスタ12-2の出力を切替スイッチ15aに入力している。そして、この切替スイッチ15aの出力と最後段のレジスタ12-7の出力を排他的論理和回路14bに入力し、この排他的論理和回路14bの出力を先頭のレジスタ12-1に入力するようにしている。切替スイッチ15aは、初めレジスタ12-1の出力を選択しており、レジスタ12-1～12-7のビット数に応じた乱数列の一周期分の回数だけLFSRがシフトした後に、レジスタ12-2の出力を選択し、この状態で乱数列の一周期分の回数だけLFSRがシフトした後に、再びレジスタ12-1の出力を選択する。このようにして、乱数の周期を約2倍にすることができる。

【0008】

5

【発明が解決しようとする課題】以上のようにして従来の疑似乱数発生回路では、乱数性を高めているが、LFSRで得られる乱数系列を著しく乱すものではないので、生成された乱数列とその疑似乱数発生回路を動作させている周辺の回路動作との比較検討により、疑似乱数発生回路の構成が判明してしまうという問題点があった。その結果、このような疑似乱数発生回路から生成される乱数列を暗号アルゴリズムのシードとして利用していると、暗号生成回路の出力である暗号コードと解析した乱数系列とにより、暗号化する前の平文が比較的容易に解読されてしまうという問題点があった。本発明は、上記課題を解決するためになされたもので、少ないビット数のLFSRで高い乱数性が得られ、かつ生成された乱数列から回路構成を解析することのできない疑似乱数発生回路を提供することを目的とする。

【0009】

【課題を解決するための手段】本発明の疑似乱数発生回路は、請求項1に記載のように、生成する乱数のビット幅分のレジスタと少なくとも1ビットの冗長レジスタから複数のレジスタが構成され、シフトクロックに応じてシフト動作を行うリニアフィードバックシフトレジスタと、冗長レジスタの出力値に応じて複数の内部クロックから1つを選択し、これをシフトクロックとして出力する選択回路とを有するものである。このように、リニアフィードバックシフトレジスタ中に冗長レジスタを設け、選択回路が冗長レジスタの出力値に応じて複数の内部クロックから1つを選択してシフトクロックとして出力することにより、見かけ上の周期がレジスタ及び冗長レジスタのビット数で決定される周期よりも長くなる疑似乱数発生回路を得ることができる。

【0010】また、請求項2に記載のように、生成する乱数のビット幅分のレジスタと少なくとも1ビットの冗長レジスタから複数のレジスタが構成され、シフトクロックに応じてシフト動作を行うリニアフィードバックシフトレジスタと、冗長レジスタの出力値に応じて複数の内部クロックから1つを選択する選択回路と、内部クロックよりも高速なクロックと選択回路の出力との論理積をとり、この結果をシフトクロックとして出力する論理積回路とを有するものである。このように、リニアフィードバックシフトレジスタ中に冗長レジスタを設け、選択回路が冗長レジスタの出力値に応じて複数の内部クロックから1つを選択し、論理積回路が内部クロックよりも高速なクロックと選択回路の出力との論理積をとることにより、見かけ上の周期がレジスタ及び冗長レジスタのビット数で決定される周期よりも長くなる疑似乱数発生回路を得ることができる。

【0011】また、請求項3に記載のように、リニアフィードバックシフトレジスタの代わりに、生成する乱数のビット幅分のレジスタから複数のレジスタが構成され、シフトクロックに応じてシフト動作を行う第1のリ

6

ニアフィードバックシフトレジスタと、複数のレジスタ中に少なくとも1ビットの冗長レジスタを含み、シフトクロックに応じてシフト動作を行う第2のリニアフィードバックシフトレジスタとを有するものである。

【0012】

【発明の実施の形態】

実施の形態の1. 以下、本発明の実施の形態について図面を参照して説明する。図1は本発明の第1の実施の形態を示す疑似乱数発生回路のブロック図、図2はこの疑似乱数発生回路の動作を説明するためのタイミングチャート図である。図2(a)は後述するレジスタ2-1~2-7、3-1、3-2をリセットするためのリセット信号RST、図2(b)~図2(e)は内部クロックCLKa~CLKd、図2(f)はシフトクロックSCK、図2(g)は冗長レジスタ3-1、3-2の出力値d1、d2を示している。

【0013】本実施の形態の疑似乱数発生回路は、シフトクロックSCKに応じてシフト動作を行うLFSR1と、図示しないクロック発生手段から出力された内部クロックCLKa、CLKb、CLKc、CLKdから1つを選択し、これをシフトクロックSCKとして出力する選択回路となるデコーダ/マルチプレクサ5(以下、MPX5と略す)を有する。

【0014】そして、LFSR1は、生成する乱数列のビット幅分(本実施の形態では7個)だけ直列に接続されたレジスタ2-1~2-7と、このレジスタの上位側に直列に接続された、その出力が外部に読み出されることのない冗長レジスタ3-1、3-2と、レジスタ2-2、2-7の出力を入力とし、その出力をレジスタ3-1の入力にフィードバックする排他的論理和回路4とから構成されている。なお、レジスタ3-1、3-2、2-1~2-6の各出力は、次段のレジスタの入力に接続されている。

【0015】MPX5は、冗長レジスタ3-1、3-2の出力値d1、d2をデコードし、このデコード結果に基づいて内部クロックCLKa、CLKb、CLKc、CLKdから1つを選択する。本実施の形態では、冗長レジスタ3-1、3-2の出力値d1、d2がそれぞれ「0」、「0」のときは内部クロックCLKa、「0」、「1」のときは内部クロックCLKb、「1」、「0」のときは内部クロックCLKc、「1」、「1」のときは内部クロックCLKdを選択するものとする。

【0016】また、レジスタ2-1~2-7、3-1、3-2は、リセット信号RSTの入力により出力が「1」に初期設定される。そして、この初期設定後にリセットが解除されると、シフトクロックSCKの立ち上がりエッジのタイミングでシフト動作を行い、入力値をラッチする。なお、リセット信号RSTは、ハイ・アクティブであり、「1」でイネーブル(リセット)、

7

「0」でディセーブル（リセット解除）である。

【0017】こうして、レジスタ2-1～2-7の値b₁～b₇が7ビット幅の乱数列として読み出される。なお、乱数列の読み出しを連続して行っても、同じ値が読み出されることのないように、内部クロックCLK_a～CLK_dの周波数は、読み出し周波数の最高値の2倍以

各レジスタの出力値

時間	3-1 出力	3-2 出力	2-1 出力	2-2 出力	2-3 出力	2-4 出力	2-5 出力	2-6 出力	2-7 出力
t0	1	1	1	1	1	1	1	1	1
t1	0	1	1	1	1	1	1	1	1
t2	0	0	1	1	1	1	1	1	1
t3	0	0	0	1	1	1	1	1	1
t4	0	0	0	0	1	1	1	1	1
t5	1	0	0	0	0	1	1	1	1

【0019】ここで、t0は、図2に示すように、リセット信号RSTがイネーブル時の初期状態のタイミング、t1～t5は、リセット解除後のシフトクロックSCKの各立ち上がりタイミングを示す。最初に、「1」レベルのリセット信号RSTの入力により、レジスタ2-1～2-7及び冗長レジスタ3-1、3-2の出力値は、全て「1」に初期化される（タイミングt0）。

【0020】冗長レジスタ3-1、3-2の出力値d₁、d₂が「1」、「1」なので、MPX5は、図2（f）に示すように、内部クロックCLK_dを選択して、これをシフトクロックSCKとして出力する。次いで、リセット信号RSTがディセーブル、すなわち「0」になった後、シフトクロックSCKの立ち上がり（タイミングt1）で、冗長レジスタ3-1、3-2及びレジスタ2-1～2-7はシフト動作を行う。

【0021】これにより、冗長レジスタ3-1、3-2の出力値d₁、d₂が「0」、「1」となるので、MPX5は、内部クロックCLK_bを選択して、これをシフトクロックSCKとして出力する。続いて、このクロックSCKの立ち上がり（タイミングt2）で、冗長レジスタ3-1、3-2及びレジスタ2-1～2-7はシフト動作を行う。その結果、冗長レジスタ3-1、3-2の出力値d₁、d₂が「0」、「0」となるので、MPX5は、内部クロックCLK_aを選択して、これをシフトクロックSCKとして出力する。

【0022】同様の動作が繰り返されてシフトクロックSCKの立ち上がり（タイミングt5）で、シフト動作が行われると、冗長レジスタ3-1、3-2の出力値d₁、d₂が「1」、「0」となるので、MPX5は、内部クロックCLK_cを選択する。以下、同様の動作が繰り返される。

8

上に設定される。次に、冗長レジスタ3-1、3-2及びレジスタ2-1～2-7の出力値の時系列的な変化を表1に示す。

【0018】

【表1】

【0023】本実施の形態のLFSR1を9ビット構成のLFSRとして考えると、乱数列の最大周期は $2^9 - 1$ であり、冗長レジスタ3-1、3-2の2ビットをマスクして考えると、 $2^9 - 1$ 周期の間にレジスタ2-1～2-7がとり得る値の組み合わせは $2^7 \times 4 - 1$ である。ただし、 $2^9 - 1$ 周期の間に 2^7 周期が規則的に現れる訳ではないので、レジスタ2-1～2-7から読み出される7ビット幅の乱数列は、ほぼ9次の線形最大周期 $2^9 - 1$ に近い周期を有すると考えることができる。

【0024】そして、シフトクロックSCKが次々と変化する図1の疑似乱数発生回路から乱数列を読み出す読み出し回路（例えば、暗号生成回路）は、通常、一定の読み出しクロックで読み出し動作を行うのであるから、この読み出し回路から見た乱数列の見かけ上の周期は、LFSR1のビット数で決定される周期 $2^9 - 1$ よりも長くなる。

【0025】また、本実施の形態では、冗長レジスタ3-1、3-2の出力値に基づきシフトクロックSCKが次々と変化するため、生成される7ビット幅の乱数列から疑似乱数発生回路の構成を解明しようと試みるものがあつたとしても、非常に困難である。加えて、シフトクロックSCKを選択するための冗長レジスタ3-1、3-2の出力値を直接読み出すことはできないので、さらに回路構成の解明を困難なものとしている。

【0026】なお、本実施の形態では、排他的論理和回路4の一方の入力にレジスタ2-2の出力を接続しているが、これに限るものではない。ただし、上記最大周期が得られるような位置のレジスタ出力を排他的論理和回路4の入力とすることが望ましい。

【0027】実施の形態の2. 図3は本発明の他の実施の形態を示す疑似乱数発生回路のブロック図、図4はこ

の疑似乱数発生回路の動作を説明するためのタイミングチャート図であり、図1、図2と同一の構成には同一の符号を付してある。図4(a)はリセット信号RST、図4(b)は内部クロックCLKa~CLKdよりも高速なクロックCLKe、図4(c)~図4(f)は内部クロックCLKa~CLKd、図2(g)はMPX5の出力MC、図4(h)は論理積回路6から出力されたシフトクロックSCK、図4(i)は冗長レジスタ3-1, 3-2の出力値d1, d2を示している。

【0028】本実施の形態の疑似乱数発生回路は、図1のMPX5の後に、内部クロックCLKa~CLKdよりも高速なクロックCLKeとMPX5の出力MCとの論理積をとり、この結果をシフトクロックSCKとして出力する論理積回路6を設けたものである。クロックCLKeは、内部クロックCLKa, CLKb, CLKc, CLKdに比して十分速い周波数(最低でも3~4倍)であるとする。なお、クロックCLKeは、内部クロックCLKa~CLKdと同期していなくてもよい。非同期の場合には、シフトクロックSCKの不規則性がより高まることになり、結果として乱数列の不規則性をより高めることができる。

【0029】レジスタ2-1~2-7、冗長レジスタ3-1, 3-2、排他的論理和回路4、MPX5の動作は、実施の形態の1と同様であるが、MPX5によって選択された内部クロックは、直接LFSR1のシフトクロックとはならず、論理積回路6で高速クロックCLKeと論理積をとられた後、シフトクロックSCKとなる(図4(h))。すなわち、MPX5が選択した内部クロックCLKa~CLKdの何れか1つが「1」の間、クロックCLKeによるLFSR1のシフト動作が行われる。

【0030】クロックCLKeをより高速なクロック源からとることにより、単位時間あたりのLFSR1のシフト回数は増すことになり、これは、周期的に乱数列を読み出す動作に対して同じ値が読み出される確率が高まることになるので、相対的により乱数性が高まっているといえる。

【0031】なお、乱数列を出力するレジスタのビット数、冗長レジスタのビット数およびその位置、クロックの種類は、必要とする乱数列のビット数、許容される回路規模、疑似乱数の周期性の長さなどに基づいて任意に設定可能であり、ここにあげた2つの実施の形態に限定されるものではない。例えば、冗長レジスタのビット数は1ビット以上であればよく、冗長レジスタを設ける位置もLFSR内であればどこに設けてもよい。また、同一のシフトクロックで動作する第1、第2のLFSRの2つのLFSRを設けて、第1のLFSRで乱数列を生成し、第2のLFSR内の冗長レジスタの出力でMPXを切替制御するようにしてもよい。

【0032】

【発明の効果】本発明によれば、請求項1に記載のように、リニアフィードバックシフトレジスタ中に冗長レジスタを設け、選択回路が冗長レジスタの出力値に応じて複数の内部クロックから1つを選択してシフトクロックとして出力することにより、任意のビット数のリニアフィードバックシフトレジスタで得られる最大の乱数列

(M系列)を時系列的に乱すことができ、乱数列の見かけ上の周期がレジスタ及び冗長レジスタのビット数で決定される周期よりも長くなる疑似乱数発生回路を得ることができる。さらに、直接読み出すことができない冗長レジスタの出力値によりクロック選択を行い、シフトクロックを次々と変化させるので、小規模な回路の追加で、疑似乱数発生回路の構成又は乱数列の周期の解明を困難なものとすることができる。その結果、少ないビット数のリニアフィードバックシフトレジスタで高い乱数性が得られ、かつ生成された乱数列から回路構成を解析することのできない疑似乱数発生回路を実現することができる。

【0033】また、請求項2に記載のように、リニアフィードバックシフトレジスタ中に冗長レジスタを設け、選択回路が冗長レジスタの出力値に応じて複数の内部クロックから1つを選択し、論理積回路が内部クロックよりも高速なクロックと選択回路の出力との論理積をとることにより、任意のビット数のリニアフィードバックシフトレジスタで得られる最大の乱数列(M系列)を時系列的に乱すことができ、乱数列の見かけ上の周期がレジスタ及び冗長レジスタのビット数で決定される周期よりも長くなる疑似乱数発生回路を得ることができる。さらに、直接読み出すことができない冗長レジスタの出力値によりクロック選択を行い、シフトクロックを次々と変化させるので、小規模な回路の追加で、疑似乱数発生回路の構成又は乱数列の周期の解明を困難なものとすることができる。その結果、少ないビット数のリニアフィードバックシフトレジスタで高い乱数性が得られ、かつ生成された乱数列から回路構成を解析することのできない疑似乱数発生回路を実現することができる。

【0034】また、請求項3に記載のように、第1のリニアフィードバックシフトレジスタと第2のリニアフィードバックシフトレジスタを設けることにより、任意のビット数の第1のリニアフィードバックシフトレジスタで得られる最大の乱数列(M系列)を時系列的に乱すことができ、乱数列の見かけ上の周期が第1のリニアフィードバックシフトレジスタのビット数で決定される周期よりも長くなる疑似乱数発生回路を得ることができる。さらに、直接読み出すことができない冗長レジスタの出力値によりクロック選択を行い、シフトクロックを次々と変化させるので、小規模な回路の追加で、疑似乱数発生回路の構成又は乱数列の周期の解明を困難なものとすることができる。その結果、少ないビット数のリニアフィードバックシフトレジスタで高い乱数性が得られ、か

つ生成された乱数列から回路構成を解析することのできない疑似乱数発生回路を実現することができる。

【図面の簡単な説明】

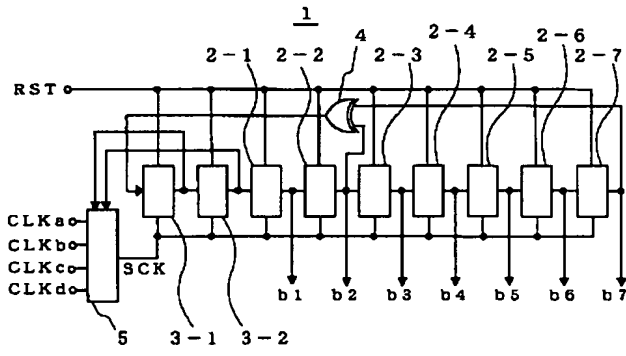
【図1】 本発明の第1の実施の形態を示す疑似乱数発生回路のブロック図である。

【図2】 図1の疑似乱数発生回路の動作を説明するためのタイミングチャート図である。

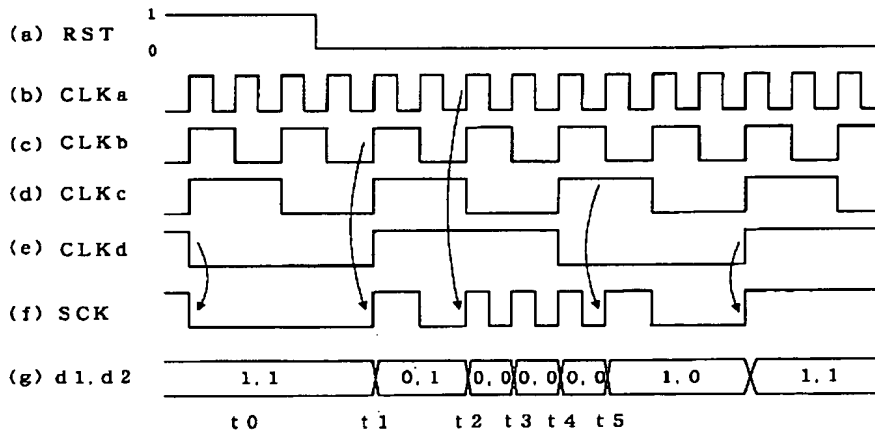
【図3】 本発明の他の実施の形態を示す疑似乱数発生回路のブロック図である。

【図4】 図3の疑似乱数発生回路の動作を説明するためのタイミングチャート図である。

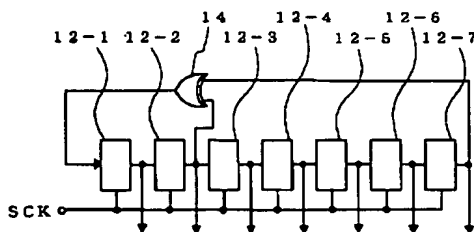
【図1】



【図2】



【図5】



【図5】 従来の疑似乱数発生回路のブロック図である。

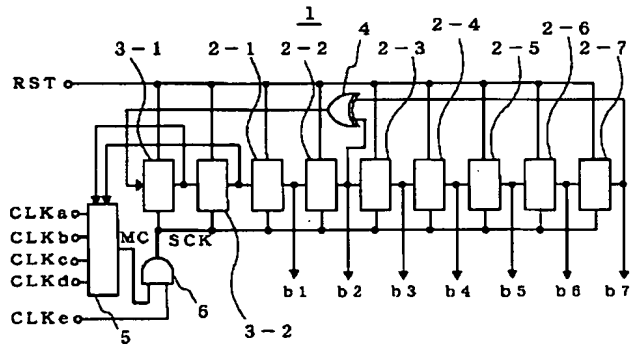
【図6】 従来の疑似乱数発生回路のブロック図である。

【図7】 従来の疑似乱数発生回路のブロック図である。

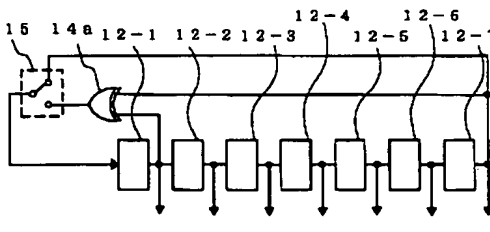
【符号の説明】

1…LFSR、2-1～2-7…レジスタ、3-1、3-2…冗長レジスタ、4…排他的論理和回路、5…MPX、6…論理積回路。

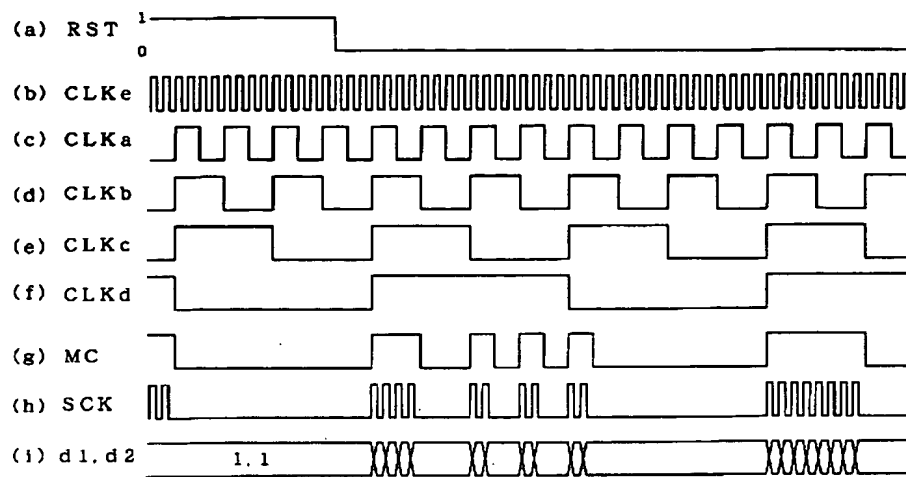
【図3】



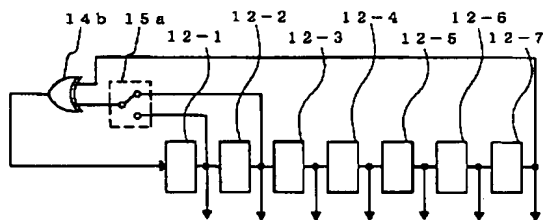
【図6】



【図4】



【図7】



フロントページの続き

(56) 参考文献 特開 昭54-41036 (J P, A)
特開 平4-313119 (J P, A)

(58) 調査した分野(Int. Cl.⁶, D B 名)
G06F 7/58
G09C 1/00 650
H03K 3/84